

Aussagenlogik

- Syntax
- Semantik
- Formeln, Modelle, Tautologien und Anwendungen
- Folgerungen, Wissen
- Syntaktisch besondere Formeln und Formelgraphen, wichtige Algorithmen
- **Axiomatiken, Kalküle**

Jeder korrekte axiomatisch-deduktive Kalkül

... verwendet:

- Junktorenbasis ***Ju***
... definiert „repräsentative“ Formelmengemenge **Form(*Ju*)**:
 - sie produzieren alle Wahrheitswerteverläufe, und
 - zu jeder AL-Formel gibt es eine äquivalente *Ju*-Formel.
- Menge ***Ax*** von **Axiomen**,
ausgewählte AL-Tautologien über *Ju*
- Menge ***Reg*** von **Inferenz-** oder **Ableitungsregeln**,
ausgewählte AL-Folgerungen aus endlichen Formelmengen
 $\{\varphi_1, \dots, \varphi_n\} \models \psi$,
allesamt *Ju*-Formeln.

Ableitungsschritt

Anwendung eines Axioms ψ bedeutet:

- Wahl einer Substitution $z = A_1, \dots, A_k / \pi_1, \dots, \pi_k$ und
- Aufnahme von $\psi_{[z]}$ in die Menge der abgeleiteten Formeln.
- Man schreibt auch $\vdash_{\psi} \psi_{[z]}$.

Anwendung einer Regel $R: \{\varphi_1, \dots, \varphi_n\} \models \psi$ bedeutet:

- Wahl einer Substitution $z = A_1, \dots, A_k / \pi_1, \dots, \pi_k$, derart, dass $\varphi_{1[z]}, \dots, \varphi_{n[z]}$ bereits abgeleitet sind, und
- Aufnahme von $\psi_{[z]}$ in die Menge der abgeleiteten Formeln.
- Man schreibt auch $\varphi_{1[z]}, \dots, \varphi_{n[z]} \vdash_R \psi_{[z]}$.

Anwendungsbeispiel: Ist $R: A \wedge B \models A \vee B$ und $z = A, B / C, D \rightarrow E$ und die Formel $C \wedge (D \rightarrow E)$ bereits abgeleitet, so erzeugt ein Ableitungsschritt mit R die Formel $C \vee (D \rightarrow E)$: $C \wedge (D \rightarrow E) \vdash C \vee (D \rightarrow E)$

Regeln

Axiome sind praktisch spezielle Regeln $\emptyset \models \psi$ mit leerer Menge von Prämissen.

Wir reden daher jetzt oft einfach nur noch von **Regeln**.

Die wichtigste Inferenzregel ist der Modus Ponens

$$\boxed{\text{MP} : A, A \rightarrow B \models B.}$$

Vollständigkeit

Den Kalkül nennt man **vollständig**, wenn es möglich ist, durch wiederholte Anwendung der Axiome und Regeln

- **alle Tautologien** über JU und
- bei Vorgabe einer Wissensbasis $M \subseteq \text{Form}(JU)$ **alle Folgerungen** aus M (über JU) abzuleiten.

Ableitbare Formeln

Aus Formelmenge ableitbare Formeln:

Induktiv φ ist mittels eines Kalküls (Ju, Reg) **aus** $M \subseteq \text{Form}(Ju)$ **ableitbar**, wenn:

- $\varphi \in M$ oder
- es existiert Menge M' aus M ableitbarer Formeln und Regel $R \in Reg$ derart, dass φ mittels R (und Substitution) in einem Schritt aus M' ableitbar ist, $M' \vdash_R \varphi$.

Iterativ **Menge** der mittels eines Kalküls (Ju, Reg) **aus** $M \subseteq \text{Form}(Ju)$ **ableitbaren** Formeln:

- $\text{Abl}_{Reg}^0(M) := M$
- $\text{Abl}_{Reg}^{n+1}(M) := \text{Abl}_{Reg}^n(M) \cup \bigcup_{R \in Reg} \{ \varphi \in \text{Form} \mid \text{Abl}_{Reg}^n(M) \vdash_R \varphi \}$
- $\text{Abl}_{Reg}(M) := \bigcup_{n=1}^{\infty} \text{Abl}_{Reg}^n(M)$.

Ableitung, Beweis

Ableitung/Beweis einer Formel φ (aus M mit Reg) :=

endliche Folge $\varphi_1, \dots, \varphi_n$ mit $\varphi = \varphi_n$ und derart,
dass jedes φ_k in M
oder aus davorstehenden Formeln unmittelbar ableitbar ist:
$$\varphi_k \in \text{Abl}_{Reg}^1(\{\varphi_1, \dots, \varphi_{k-1}\}).$$

Kalkülbeispiele (1)

Hilbert-Ackermann	
Junktorenbasis	\neg, \vee
Axiome	$\neg(A \vee A) \vee A$ $\neg(A \vee B) \vee (B \vee A)$ $\neg A \vee (A \vee B)$ $\neg(\neg A \vee B) \vee (\neg(C \vee A) \vee (C \vee B))$
Inferenzregeln	Modifizierter Modus Ponens MMP = $\frac{A, \neg A \vee B}{B}$

Mendelson	
Junktorenbasis	\neg, \rightarrow
Axiome	$A \rightarrow (B \rightarrow A)$ $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$ $(\neg B \rightarrow \neg A) \rightarrow ((\neg B \rightarrow A) \rightarrow B)$
Inferenzregeln	Modus Ponens

Beide sind **ableitungs-** (und beweis-) **korrekt** und **vollständig**.

Kalkülbeispiele (2)

Mit Geschick **reicht ein einziges** (recht langes) **Axiom**.

Es gab schon „sportliche Wettläufe“ um das jeweils **kürzeste** einzige Axiom in einer Junktorenbasis.

Andere Axiomensysteme spendieren **mehr Axiome**:

Hilbert-Bernays, Kleene, de Swart, ...

Beweisbeispiele (1)

Beweis = Ableitung aus den Axiomen!

$A \rightarrow A$ im Mendelson-Kalkül

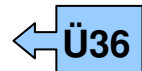
- | | |
|--|----------------------------------|
| 1. $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$ | Axiom |
| 2. $(A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$ | 1, $[B, C / A \rightarrow A, A]$ |
| 3. $A \rightarrow (B \rightarrow A)$ | Axiom |
| 4. $A \rightarrow ((A \rightarrow A) \rightarrow A)$ | 3, $[B / A \rightarrow A]$ |
| 5. $((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$ | 2, 4, MP |
| 6. $A \rightarrow (A \rightarrow A)$ | 3, $[B / A]$ |
| 7. $A \rightarrow A$ | 5, 6, MP |

Beweisbeispiele (2)

$A \rightarrow A$ (d.h. $\neg A \vee A$) im Hilbert-Ackermann-Kalkül

- | | | |
|----|--|-------------------------------|
| 1. | $\neg(\neg A \vee B) \vee (\neg(C \vee A) \vee (C \vee B))$ | Axiom |
| 2. | $\neg(\neg A \vee B) \vee (\neg(\neg C \vee A) \vee (\neg C \vee B))$ | 1, $C / \neg C$ |
| 3. | $\neg A \vee (A \vee B)$ | Axiom |
| 4. | $\neg A \vee (A \vee A)$ | 3, B / A |
| 5. | $\neg(\neg(A \vee A) \vee A) \vee (\neg(\neg A \vee (A \vee A)) \vee (\neg A \vee A))$ | 2, $A, B, C / A \vee A, A, A$ |
| 6. | $\neg(\neg A \vee (A \vee A)) \vee (\neg A \vee A)$ | 4,5,MMP |
| 7. | $\neg A \vee A$ | 4,6,MMP |

Leichter nachzuprüfen als darauf zu kommen!



Berechtigte Fragen (1)

Wozu Kalküle und Beweise?
Wir haben doch unsere Wahrheitstafeln und sonstigen Algorithmen!



(1) **Komplexität**

Man beweist lieber $(A \wedge B \wedge C \wedge D \wedge E \wedge F \wedge G) \rightarrow A$ in wenigen Schritten im Kalkül als mittels Wahrheitstafel mit 128 Zeilen und 1792 Feldern.

(2) **Berechenbarkeit**

In der vollen Prädikatenlogik handeln die „Formeln“ von Eigenschaften von potentiell **unendlich vielen verschiedenen Objekten**. Die kann man **nicht** mehr alle in einer **Tabelle** erfassen und durchrechnen.

Da gibt es (beweisbar!) **keinen** sicher terminierenden **Algorithmus** zur Überprüfung der Erfüllbarkeit etc. – wir **sind auf Beweise angewiesen**.



Berechtigte Fragen (2)

**Na gut, dann umgekehrt:
Wozu diese ganzen Wahrheitstafeln und sonstigen Algorithmen?**



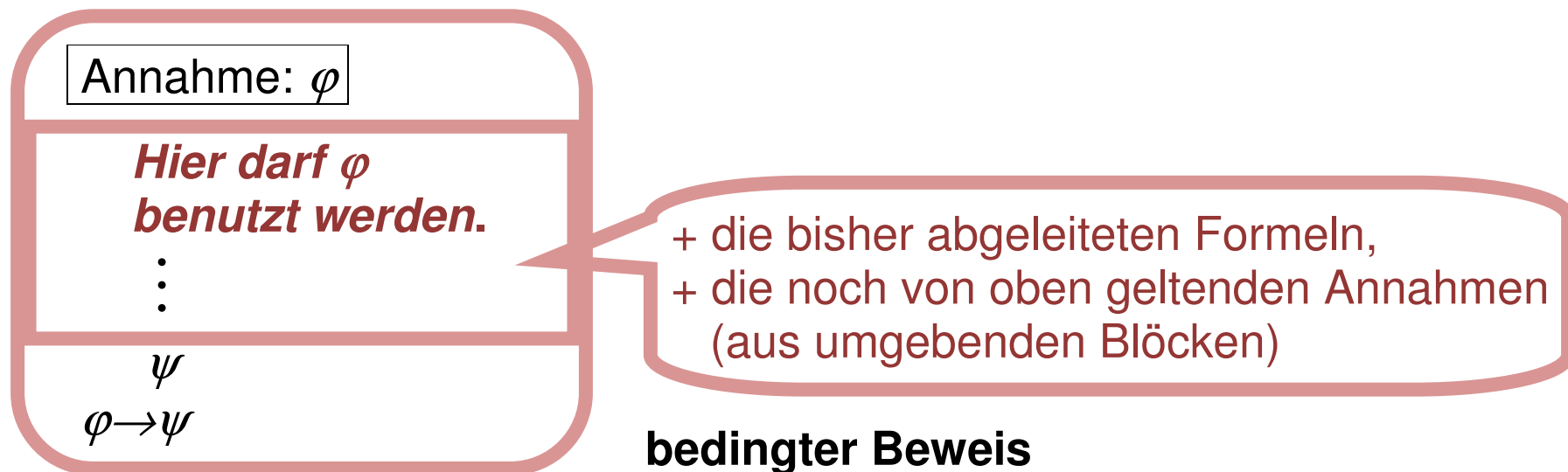
In vielen praktischen Fragen gelingt es, das Ganze in Aussagenlogik auszudrücken. Und dann kann man zum Glück den Computer die algorithmische Arbeit erledigen lassen.



Natürliches Schließen und unser Werkzeugkasten

In den 1930er Jahren erweiterte Gerhard Gentzen die axiomatischen Kalküle gewissermaßen um das Deduktionstheorem und erhielt so seinen (formalen) **Kalkül des natürlichen Schließens**, der weitgehend das formlose Beweisen in Mathematikbüchern streng formal nachbildet.

Seine Beweise sind nicht reine **Folgen** von Formeln, wie im Vorigen, sondern haben teilweise eine **Blockstruktur**:



GNS-Beispiel

Ableitung von $(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$

nach unserer GNS-Definition, annotiert,
in einer Baumschreibweise mit Einrückung
(traditionelle Schreibweise anders):

Nr.	Formel	Regel,-Pr.
1	Ann: $A \rightarrow B$	AE
2	Ann: $B \rightarrow C$	AE
3	Ann: A	AE
4	B	FB,1,3
5	C	FB,2,4
6	$A \rightarrow C$	FE,3,5
7	$(B \rightarrow C) \rightarrow (A \rightarrow C)$	FE,2,6
8	$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$	FE,1,7

GNS-Beispiel, historisch

Ableitung von $(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$

traditionelle Schreibweise

$$\begin{array}{r}
 \frac{[A]_1 \quad [A \rightarrow B]_3}{B} \text{ FB} \qquad [B \rightarrow C]_2 \\
 \hline
 \qquad \qquad \qquad C \text{ FB} \\
 \qquad \qquad \qquad \hline
 \qquad \qquad \qquad A \rightarrow C \text{ FE}_1 \\
 \qquad \qquad \qquad \hline
 \qquad \qquad (B \rightarrow C) \rightarrow (A \rightarrow C) \text{ FE}_2 \\
 \qquad \qquad \hline
 (A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C)) \text{ FE}_3
 \end{array}$$

Beispiel in „Werkzeugkastenversion“

Zeige $(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$

1.		$A \rightarrow B$				Ann
					○ Zeige $(B \rightarrow C) \rightarrow (A \rightarrow C)$	
2.					$B \rightarrow C$	Ann
					Zeige $(A \rightarrow C)$	
3.					A	Ann
4.					B	MP,1,3
5.					C	MP,2,4
6.					$A \rightarrow C$	BB
7.					○ $(B \rightarrow C) \rightarrow (A \rightarrow C)$	BB
8.					$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$	BB

Zielfor-
mulierung
→ begin

Ziel
erreicht
→ end

Unser Werkzeugkasten (erweitertes GNS) wird noch **weitere Regeln** enthalten, und die damit gebauten Beweise werden sehr „natürlich“ und doch **exakt** sein.

Werkzeugkasten – Beweisaufbau – Zeilentypen

ohne **Ableitungsbegründung**:

1. Zuerst die **Prämissen**

Ausgangsannahmen, aus denen gefolgert werden soll – sofern vorhanden: keine bei Beweisen von Tautologien:

φ Gegeben

2. **Zielformeln** (eine erste unmittelbar nach den Prämissen): **Zeige φ**

3. ad hoc **angenommene Formeln**, für IB/BB-Blöcke:

φ Annahme

mit **Ableitungsbegründung**:

4. **abgeleitete Formeln**:

speziell: Erfüllungszeilen

φ Regel, Prämissennummer(n)

φ Beweistyp (DB/IB/BB)

Alle (außer Zielformeln) sind jeweils durchnummeriert – wegen späterer Verweise als Prämissennummern.

Werkzeugkasten – Beweisaufbau – Blöcke

- Auf die Prämissen folgt der **Haupt-Block**.
- 5. Ein **Block** beginnt mit einer **Zielzeile** (**Zeige** φ),
dann kommt (eingerückt) der **Blockkörper**,
Die **letzte** Formel im eingerückten Blockkörper muss jeweils **abgeleitet** sein.
am Ende (nicht mehr eingerückt) die Erfüllungszeile φ .
- Es gibt 4 Blockschemata, den 4 Beweismethoden entsprechend,
→ Tabelle.
- Im Blockkörper stehen **angenommene** Formeln und Erfüllungszeilen nur dort, wo im Blockschema gezeigt (oder entsprechend in Unterblöcken), abgeleitete Formeln und **Unterblöcke (Zwischenbeweise)** aber nach Belieben.

Wie wird abgeleitet?

- per **Blockschema/Beweismethode**

oder

- per **Ableitungsregeln/Schlussregeln**

→ Tabelle

In der Regelanwendung verfügbare Voraussetzungen (Prämissen) sind frühere Formeln aus dem laufenden oder dessen umgebenden Blöcken.

Beweis-Methoden (1)

a) Direkter Beweis

Blockbeginn: Zeige φ .

Sobald im **Blockkörper** φ abgeleitet, ...

Blockende: Erfüllungszeile φ **DB**.

... dienen der Zerlegung in Teilaufgaben.

b) Bedingter Beweis

Blockbeginn: Zeige $\varphi \rightarrow \psi$,

Annahmezeile φ **Ann**

Sobald im gleichen Block ψ abgeleitet, ...

Blockende: Erfüllungszeile $\varphi \rightarrow \psi$ **BB**.

Direkter Beweis:

Zeige φ

| \vdots

(| φ) *weglassbar s.u.*

φ **DB**

Bedingter Beweis:

Zeige $\varphi \rightarrow \psi$

| φ **Ann**

| \vdots

| ψ

$\varphi \rightarrow \psi$ **BB**

(Zwischen) Beweis-Methoden (2)

c) Indirekter Beweis 1

Blockbeginn: Zeige φ ,

im Blockkörper unmittelbar gefolgt von $\neg\varphi$ **Ann**

Sobald im Blockkörper \perp (Widerspruch) abgeleitet, ...

Blockende: φ **IB1**

d) Indirekter Beweis 2

Blockbeginn: Zeige $\neg\varphi$,

im Blockkörper unmittelbar gefolgt von φ **Ann**

Sobald im gleichen Block \perp (Widerspruch) abgeleitet, ...

Blockende: $\neg\varphi$ **IB2**

Indirekter Beweis 1:

Zeige φ

| $\neg\varphi$ Ann

| \vdots

| \perp

φ IB1

Indirekter Beweis 2:

Zeige $\neg\varphi$

| φ Ann

| \vdots

| \perp

$\neg\varphi$ IB2

Werkzeugkasten – Schlussregeln (1)

Oder-Einführung	OE $\frac{\varphi}{\varphi \vee \psi}, \frac{\psi}{\varphi \vee \psi}$	Oder-Benutzung 1	OB ₁ $\frac{\varphi \vee \psi, \neg \varphi}{\psi}, \frac{\varphi \vee \psi, \neg \psi}{\varphi}$
Und-Einführung	UE $\frac{\varphi, \psi}{\varphi \wedge \psi}$	Oder-Benutzung 2	OB ₂ $\frac{\varphi \vee \psi, \varphi \rightarrow \rho, \psi \rightarrow \rho}{\rho}$
Und-Benutzung	UB $\frac{\varphi \wedge \psi}{\varphi}, \frac{\varphi \wedge \psi}{\psi}$	Wiederholung	WDH $\frac{\varphi}{\varphi}$
Doppelte Negations-Einführung	DNE $\frac{\varphi}{\neg \neg \varphi}$	Doppelte-Negations-Benutzung	DNB $\frac{\neg \neg \varphi}{\varphi}$
Gdw-Einführung	GE $\frac{\varphi \rightarrow \psi, \psi \rightarrow \varphi}{\varphi \leftrightarrow \psi}$	Gdw-Benutzung links/ rechts	GB $\frac{\varphi \leftrightarrow \psi}{\varphi \rightarrow \psi}, \frac{\varphi \leftrightarrow \psi}{\psi \rightarrow \varphi}$
Widerspr.-Einführung	WE $\frac{\varphi, \neg \varphi}{\perp}$	Widerspruch-Benutzung	WB $\frac{\perp}{\varphi}$
Folgerungs-Benutzung Modus Ponens	MP $\frac{\varphi, \varphi \rightarrow \psi}{\psi}$	Folgerungs-Benutzung Modus Tollens	MT $\frac{\varphi \rightarrow \psi, \neg \psi}{\neg \varphi}$

Werkzeugkasten – Schlussregeln (2)

Nicht-Und-Benutzung	NUB $\frac{\neg(\varphi \wedge \psi)}{\varphi \rightarrow \neg\psi}, \frac{\neg(\varphi \wedge \psi)}{\psi \rightarrow \neg\varphi}$	Nicht-Oder-Benutzung	NOB $\frac{\neg(\varphi \vee \psi)}{\neg\varphi}, \frac{\neg(\varphi \vee \psi)}{\neg\psi}$
Nicht-Folgerungs-Benutzung	NFB $\frac{\neg(\varphi \rightarrow \psi)}{\varphi \wedge \neg\psi}$	Nicht-Gdw-Benutzung	NGB $\frac{\neg(\varphi \leftrightarrow \psi)}{\neg\varphi \leftrightarrow \psi}, \frac{\neg(\varphi \leftrightarrow \psi)}{\varphi \leftrightarrow \neg\psi}$

Weitere Regeln sind aus Äquivalenz- und Implikation-Tautologien **herleitbar**.

Modularität: Sinnvoll ist in der **Praxis** auch das Einfügen von *anderswo bewiesenen* Tautologien oder Folgerungen aus M (mit einer Quellenangabe an Stelle der **Ableitungsbegründung**).

Autoren von Mathematikbüchern zitieren z.B. oft früher (im gleichen Buch oder anderswo) bewiesene „Sätze“ in Beweisen späterer Sätze, anstatt deren komplette Beweise in den neuen Beweis einzubauen.

Werkzeugkasten – 3 Beweisstrategien

Zeige $\varphi \wedge \psi$ Zeige φ \vdots φ Zeige ψ \vdots ψ $\varphi \wedge \psi$	Zeige $\varphi \leftrightarrow \psi$ Zeige $\varphi \rightarrow \psi$ \vdots $\varphi \rightarrow \psi$ Zeige $\psi \rightarrow \varphi$ \vdots $\psi \rightarrow \varphi$ $\varphi \leftrightarrow \psi$	Zeige $\varphi \vee \psi$ $\neg(\varphi \vee \psi)$ AE $\neg\varphi$ NOB $\neg\psi$ NOB \vdots \perp $\varphi \vee \psi$ IB1
UE	GE	

Werkzeugkasten – Nutzen

Satz: Der **Werkzeugkasten** für **Aussagenlogik** ist (ableitungs- und beweis-) **korrekt** und **vollständig**.

Der **Werkzeugkasten formalisiert** die **manuell** üblichen Beweise und macht sie dadurch **maschinell überprüfbar**.

Aber er führt (wie manuelle Beweisversuche) **nicht zwingend** zum Beweis einer korrekten Tautologie oder Folgerung.

Er verwendet implizit das **Deduktionstheorem** (siehe bedingter Beweis). Dies erlaubt **kürzere Beweise** als z.B. nur mit Axiomen und Modus Ponens.

Vergleich axiomatischer und Werkzeugkasten-Beweis

Erinnerung:

$A \rightarrow A$ im Mendelson-Kalkül

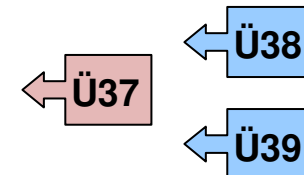
- | | |
|--|----------------------------------|
| 1. $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$ | Axiom |
| 2. $(A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$ | 1, $[B, C / A \rightarrow A, A]$ |
| 3. $A \rightarrow (B \rightarrow A)$ | Axiom |
| 4. $A \rightarrow ((A \rightarrow A) \rightarrow A)$ | 3, $[B / A \rightarrow A]$ |
| 5. $((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$ | 2, 4, MP |
| 6. $A \rightarrow (A \rightarrow A)$ | 3, $[B / A]$ |
| 7. $A \rightarrow A$ | 5, 6, MP |

Neu:

$A \rightarrow A$ – mit Werkzeugkasten

Zeige $A \rightarrow A$

- | | |
|----------------------|--------|
| 1. A | Ann |
| 2. A | Wdh, 1 |
| 3. $A \rightarrow A$ | BB |

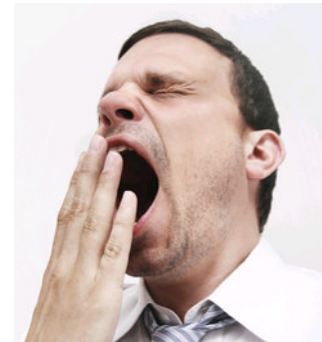


Exkurs: Interessante mathematische Sätze über AL



Mathematiker

- **Interpolationssätze**
- **Kompaktheitssätze**



Nichtmathematiker

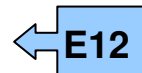
Interpolationssätze der AL

Craigs Interpolationssatz für AL

Wenn für zwei Formeln φ, ψ gilt: $\models \varphi \rightarrow \psi$, dann

- kommt entweder eine Aussagevariable P sowohl in φ als auch in ψ vor, und dann existiert auch eine Formel π , deren sämtliche Aussagevariablen sowohl in φ als auch in ψ vorkommen, derart dass $\models \varphi \rightarrow \pi$ und $\models \pi \rightarrow \psi$.
- oder sie haben keine Aussagevariable gemeinsam, und $\models \neg\varphi$ oder $\models \psi$.

Beweis (mit **Konstruktion** für ein π): Wikipedia (englisch) – Craig interpolation

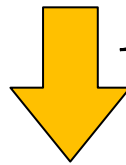


Lyndons Interpolationssatz für AL

- Wenn sich zwei Theorien S, T widersprechen, d.h. wenn für zwei Theorien S, T $\text{Theo}(S \cup T)$ unerfüllbar ist, dann existiert eine Formel φ , deren sämtliche Aussagevariablen sowohl in S als auch in T vorkommen und derart dass $S \models \varphi$ und $T \models \neg\varphi$... (+ weitere Eigenschaften von φ)

Kompaktheitssätze der AL

- Eine Formelmengemenge M ist **erfüllbar** genau dann, wenn **jede endliche Teilmenge von M erfüllbar** ist.



nette Übung in
Prädikatenlogik
und Mengenlehre

- Aus einer Formelmengemenge M **folgt** eine Formel ψ , $M \models \psi$, genau dann, wenn ψ bereits aus **einer endlichen Teilmenge** $N \subseteq M$ folgt: $N \models \psi$.

Ein möglicher Beweisweg der **oberen Aussage** für **abzählbare M** verwendet **Königs Lemma**.

Für **beliebige M** aber verwendet man das **Lemma von Zorn**:

In jeder nicht-leeren partiellen Ordnung,
in der jede Kette nach oben beschränkt ist,
existiert ein maximales Element.

Das geht aber nur in einer Mengenlehre mit **Auswahlaxiom**.

Das Auswahlaxiom kommt den meisten intuitiv **selbstverständlich** vor, hat aber Konsequenzen, die den meisten (zunächst?) intuitiv **falsch** vorkommen.

→ **Banach-Tarski-Paradoxon**